### Setting Up Auto Remediation for AWS Config with SSM

**Step 1: Activating AWS Config**

When activating AWS Config, you have two options:

* **Get Started**
* **1-Click Setup**

I’m selecting **Get Started** option for a more detailed setup.

**Step 2: Configuring General and Delivery Method Settings**

**General Settings:**

* **Recording strategy:**
  + Record all current and future resource types supported in this region
  + Record all current and future resource types with exclusions
  + Record specific resource types (Selected for this setup)

A screenshot of a computer

AI-generated content may be incorrect.

* **AWS Config Service Role:**
  + Create AWS Config service-linked role (Recommended if no existing role is available)

A screenshot of a computer

AI-generated content may be incorrect.

**Delivery Method:**

* **S3 Bucket for Log Storage:**
  + Create a new bucket or select an existing one (New bucket created for this setup)

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Selecting AWS Config Rules**

* We selected **ec2-imdsv2-check** to enforce IMDSv2.

*A screenshot of a computer

AI-generated content may be incorrect.*

**Reviewing and Confirming Configuration**

* Verify the selected resource types and rules.
* Click **Confirm** to complete setup.

**AWS Config Dashboard Overview**

* Displays compliance status, conformance packs, resource inventory, and usage metrics.

*A screenshot of a computer

AI-generated content may be incorrect.*

### Configuring Remediation

**Step 1: Accessing Remediation Actions**

* Navigate to **Rules** and select **ec2-imdsv2-check**.
* Click on **Actions → Manage remediation**.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 2: Setting Remediation Parameters**

* **Automatic Remediation** selected.
* **Retries:** Default values (5 retries, 60 seconds interval).
* **Remediation Action:** AWSConfigRemediation-EnforceEC2InstanceIMDSv2

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Creating an IAM Role for Remediation**

* Navigate to **IAM → Roles → Create Role**.
* Select **AWS Service → Systems Manager**.

A screenshot of a computer

AI-generated content may be incorrect.

* Create a new policy with required permissions:

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Assign the policy to the role and copy the ARN.  
  “arn:aws:iam::337909744329:role/SSMRemediationEC2inst”
* Paste the ARN in AWS Config's remediation settings.

A screenshot of a computer

AI-generated content may be incorrect.

### Launching a Non-Compliant EC2 Instance

**Step 1: Launch EC2 Instance**

* Open **EC2 Console → Launch Instance**.
* Select **Amazon Linux AMI**.

A screenshot of a computer

AI-generated content may be incorrect.

* Under **Advanced Details**, set **Metadata version** to V1 and V2 (token optional).

A screenshot of a computer

AI-generated content may be incorrect.

**Step 2: Checking Noncompliance**

* Refresh the **AWS Config Dashboard**.

A screenshot of a computer

AI-generated content may be incorrect.

* The instance appears as **Noncompliant**.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Verifying Automated Remediation**

* Refresh the dashboard after a few minutes.
* Instance metadata version is updated to **IMDSv2 Required**.

A screenshot of a computer

AI-generated content may be incorrect.

* AWS Config will eventually mark the instance as **Compliant**.

*A screenshot of a computer

AI-generated content may be incorrect.*